CLAIMS

1. A method of arranging data protection in a telecommunication system comprising a first mobile communication network wherein a first cipher key is used for ciphering traffic between a mobile station and a mobile communication network, a second mobile communication network wherein a second cipher key is used for ciphering traffic between a mobile station and a mobile communication network, and a mobile station supporting said mobile communication networks, **characterized** by

calculating said second cipher key in the first mobile communication network when the mobile station operates in the first mobile communication network,

transmitting information necessary for calculating said second cipher key from the first mobile communication network to the mobile station when the mobile station operates in the first mobile communication network, and

calculating said second cipher key at the mobile station.

2. A method as claimed in claim 1, **characterized** by

using said second cipher key for ciphering the traffic between the mobile station and the second mobile communication network if the mobile station is handed over from the first mobile communication network to the second mobile communication network during an active connection.

3. A method as claimed in claim 1 or 2, **characterized** by

transmitting said second cipher key from the first mobile communication network to the second mobile communication network,

transmitting said second cipher key calculated at the mobile station to a ciphering means of the mobile station in response to the fact that the first mobile communication network transmits a request to the mobile station for handover to the second mobile communication network, and

using said second cipher key in ciphering traffic after the handover in the mobile station and in the second mobile communication network.

4. A method as claimed in any one of the preceding claims, **characterized** by

checking, in the first mobile communication network, whether the mobile station supports the second mobile communication network,

calculating said second cipher key in the first mobile communication network in response to the fact that the mobile station supports the second mobile communication network,

transmitting a request for calculation of said second cipher key from the first mobile communication network to the mobile station, and

calculating at the mobile station said second cipher key in response to said request.

5. A method as claimed in claim 4, **characterized** by

calculating said second cipher key in the first mobile communication network in response to the fact that an identifier transmitted by the mobile station, such as an IMSI subscriber identifier, and/or a classmark identifier indicate that the mobile station supports the second mobile communication network.

6. A method as claimed in any one of the preceding claims, **characterized** by

calculating said second cipher key at a network element in the first mobile communication network, such as an authentication centre, in response to the fact that a network element of the first mobile communication network, such as a visitor location register or a home location register, comprising identifiers transmitted by the mobile station requests calculation of said second cipher key, and

transmitting said second cipher key from said network element calculating the cipher key to said network element comprising the identifiers transmitted by the mobile station.

7. A method as claimed in any one of the preceding claims, **characterized** by

the mobile station comprising a subscriber identification application, such as a USIM application, to the first mobile communication network and a subscriber identification application, such as an SIM application, to the second mobile communication network,

transmitting the information necessary for calculating said second cipher key received by the mobile station to the identification application according to the second mobile communication network.

8. A method as claimed in any one of the preceding claims, **characterized** by

calculating said second cipher key in the first mobile communication network in connection with calculating an authentication response according to the first mobile communication network and the first cipher key,

transmitting the information necessary for calculating the first cipher key and said second cipher key, such as a random-number parameter, from the first mobile communication network to the mobile station,

transmitting the necessary information at the mobile station for calculating said first and second cipher keys to the identification applications according to the first and the second mobile communication networks,

calculating said second cipher key in the identification application according to the second mobile communication network and the authentication response in the identification application according to the first mobile communication network,

transmitting said authentication response according to the first mobile communication network from the mobile station to the first mobile communication network, and

acknowledging the authentication of the mobile station to be performed for the second mobile communication network in response to the fact that the first mobile communication network accepts the authentication response transmitted by the mobile station.

9. A method as claimed in any one of claims 1 to 7, **characterized** by

determining a random-number parameter and calculating the authentication response according to the second mobile communication network in connection with calculating said second cipher key in the first mobile communication network,

transmitting a request to the mobile station for calculation of an authentication response according to the second mobile communication network,

transmitting the information necessary at the mobile station for calculating said second cipher key to the identification application according to the second mobile communication network,

calculating, in the identification application according to the second mobile communication network, the authentication response according to the second mobile communication network in connection with calculating said second cipher key,

transmitting the authentication response according to the second mobile communication network calculated at the mobile station to the first mobile communication network, and

checking said authentication response according to the second mobile communication network transmitted by the mobile station in the first mobile communication network.

10. A method as claimed in any one of claims 1 to 7, **characterized** by

calculating said second cipher key by shortening the first cipher key in the first mobile communication network and at the mobile station before the handover to the second mobile communication network takes place.

11. A method as claimed in any one of the preceding claims, **characterized** by

calculating said second cipher key in response to the fact that a decision has been made in the first mobile communication network to carry out handover to the second mobile communication network.

12. A telecommunication system comprising at least a first mobile communication network arranged to use a first cipher key for ciphering traffic between a mobile station and a mobile communication network, a second mobile communication network arranged to use a second cipher key for ciphering traffic between a mobile station and a mobile communication network, and a mobile station arranged to support said different first and second mobile communication networks, **characterized** in that

the first mobile communication network is arranged to calculate said second cipher key when the mobile station operates in the first mobile communication network,

the first mobile communication network is arranged to transmit information necessary for calculating said second cipher key from the first mobile communication network to the mobile station when the mobile station operates in the first mobile communication network, and

the mobile station is arranged to calculate said second cipher key.

13. A telecommunication system as claimed in claim 12, **characterized** in that

the mobile station and the second mobile communication network are arranged to cipher the traffic between the mobile station and the second mobile communication network by using said second cipher key if the mobile

station is handed over from the first mobile communication network to the second mobile communication network during an active connection.

14. A telecommunication system as claimed in claim 12 or 13, **characterized** in that

the first mobile communication network is arranged to transmit said second cipher key to the second mobile communication network before the handover to the second mobile communication network,

the mobile station is arranged to transmit said second cipher key calculated at the mobile station to a ciphering means of the mobile station in response to the fact that the first mobile communication network transmits a request to the mobile station for handover to the second mobile communication network, and

the mobile station and the second mobile communication network are arranged to use said second cipher key in ciphering traffic after the handover.

15. A telecommunication system as claimed in any one of claims 12 to 14, **characterized** in that

the first mobile communication network is arranged to check whether the mobile station supports the second mobile communication network on the basis of an identifier transmitted by the mobile station, such as an IMSI and/or a classmark identifier,

the first mobile communication network is arranged to calculate said second cipher key in response to the fact that the mobile station supports the second mobile communication network,

the first mobile communication network is arranged to transmit a request to the mobile station for calculation of said second cipher key, and

the mobile station is arranged to calculate said second cipher key on the basis of said request.

16. A telecommunication system as claimed in any one of claims 12 to 15, **characterized** in that

a network element comprising identifiers transmitted by the mobile station of the first mobile communication network, such as a visitor location register or a home location register, is arranged to transmit the request for calculation of said second cipher key to a network element of the first mobile communication network, such as an authentication centre,

the network element of the first mobile communication network, such as the authentication centre, is arranged to calculate said second cipher key in response to the fact that the network element comprising the identifiers transmitted by the mobile station requests calculation of said second cipher key, and

said network element calculating said second cipher key is arranged to transmit the calculated second cipher key to said network element comprising the identifiers transmitted by the mobile station.

17. A telecommunication system as claimed in any one of claims 12 to 16, **characterized** in that

the first mobile communication network is arranged to calculate said second cipher key in connection with calculation of an authentication response according to the first mobile communication network and the first cipher key,

the first mobile communication network is arranged to transmit to the mobile station information necessary for calculating the first cipher key and said second cipher key, such as a random-number parameter,

the mobile station comprises an identification application according to the first mobile communication network, such as a USIM application, and an identification application according to the second mobile communication network, such as an SIM application,

the mobile station is arranged to transmit said information necessary for calculating the first cipher key and said second cipher key to the identification applications according to the first and the second mobile communication networks,

said identification application according to the second mobile communication network is arranged to calculate said second cipher key and said identification application according to the first mobile communication network is arranged to calculate the authentication response according to the first mobile communication network, and

the mobile station is arranged to transmit the authentication response according to the first mobile communication network to the first mobile communication network.

18. A telecommunication system as claimed in any one of claims 12 to 16, **characterized** in that

the first mobile communication network is arranged to determine a random-number parameter according to the second mobile communication

network and to calculate the authentication response in connection with calculating said second cipher key,

the first mobile communication network is arranged to transmit a request to the mobile station for calculating the authentication response according to the second mobile communication network,

the mobile station comprises an identification application according to the first mobile communication network, such as a USIM application, and an identification application according to the second mobile communication network, such as an SIM application,

the mobile station is arranged to transmit the information necessary for calculating said second cipher key to the identification application according to the second mobile communication network,

the identification application according to the second mobile communication network is arranged to calculate said second cipher key and the authentication response according to the second mobile communication network substantially simultaneously,

the mobile station is arranged to transmit the authentication response according to the second mobile communication network to the first mobile communication network, and

the second mobile communication network is arranged to check the authentication response according to the second mobile communication network.